Vážené čtenářky, vážení čtenáři,

už opravdu drahnou chvíli se diskutuje o tom, že hesla sice představují pro ověřování jednoduchou metodu, která se snadno zavádí, ale z uživatelského hlediska není úplně komfortní – zvláště pokud správce takového systému nutí lidi pravidelně měnit hesla, která navíc musejí být plná speciálních znaků, jež je obtížné si zapamatovat.

Výsledkem je, že se taková opatření často obcházejí, a to především sdílením hesel, jejich použitím na více místech či třeba jejich zapisováním na papír, který je viditelný i cizím osobám.

I když už v minulosti vznikla řada iniciativ, které se snažily hesla odstranit (například implementací biometrie) nebo alespoň usnadnit jejich použití (třeba v podobě správců hesel), k nějakému zásadnímu posunu v tomto směru nedošlo. To se ale může velice brzy radikálně změnit.

Ukazují to nejnovější společné kroky tří klíčových IT gigantů – firem Apple, Google a Microsoft. Ty se totiž začátkem letošního května dohodly na tom, že ze svých platforem autentizaci pomocí hesel zcela odstraní – a to ještě v průběhu letošního roku.

Základem tohoto zásadního přechodu se mají stát standardy vytvořené organizacemi FIDO Alliance a World Wide Web Consortium. Ve své podstatě jde o podobu dvoufázové autentizace, kdy kromě vlastnictví mobilu se bude pro ověření jako druhý faktor brát PIN nebo biometrický ukazatel, tedy nejčastěji otisk prstu. Tato autentizace se přitom bude využívat jak pro aplikace, tak i pro weby.

V současnosti už zmínění dodavatelé poskytují formu dvoufaktorové autentizace, která slouží k bezheslovému ověřování, ale nejde o komplexní řešení, protože existují problémy například s nutností opětovného přihlašování na jiném zařízení. To nově už nebude nutné – po autentizaci na mobilu budou uživatelé automaticky ověřeni i pro blízké počítače bez ohledu na jejich operační systém nebo typ prohlížeče.

Usnadní se také například bankovní autentizace v případě ztráty mobilu – bude postačovat se přihlásit z nějakého jiného svého přístroje (například staršího mobilu), a obnovit tak okamžitě přístup k účtu.

Dalším významným počinem je eliminace používání jednorázových přístupových kódů zasílaných do vašeho telefonu prostřednictvím SMS, kdy kvůli útokům typu SIMjacking může docházet ke kompromitaci tohoto typu autentizace.

Aliance FIDO si od zmíněné aktivity tří gigantů slibuje zavedení skutečně bezheslového ověřování pro širokou škálu aplikací i webových stránek, přičemž pro uživatele půjde o velice jednoduchý úkon (otisk nebo PIN), který bude pro různé služby stále stejný a jenž už dnes důvěrně znají z odemykání svého mobilu.

S přáním příjemně stráveného léta třeba i nad stránkami nového Security Worldu

Pavel Louda
vedoucí projektu

Obsah